Amendments to the Specification:

Please replace the paragraph beginning on page 3, line 34, with the following amended paragraph:

-- Theoretically certificates are not context specific but in practice different uses require different certificates. E.g. standard X.509 certificate does not include e-mail address information that is required in secure electronic mail (e.g. electronic mail encrypted using Pretty Good Privacy® (PGP®) or Secure Multipurpose Internet Mail Extensions (S/MIME) techniques). Similarly other applications may need to have their own proprietary attributes included in certificates. Although this inclusion of attributes is not problematic per se, new certificates need to be created. --

Please replace the paragraph beginning on page 6, line 36, with the following amended paragraph:

-- Essentially the invention is intended for extending an entity's identity based on an existing mobile certificate and other verified and confirmed facts. The one of the most apparent and practical functions is to use this information to issue new certificates for various security/encryption uses such as secure e-mail, PGP® or S/MIME. The mobile variant of the solution, however, does not have to be as limited. Since the ability to provide confirmed facts about an entity is totally mobile, in certain situations certificates are not a key issue. Say, if mobile identity registration authority has access to Finnish Population Registry Center's database it can provide confirmed home address, marital status, or whatever is required. --

Please replace the paragraph beginning on page 8, line 5, with the following amended paragraph:

-- Referring further to figure 1 it is described one preferred solution of the present invention. This solution is described in the context of certifying a new PGP® key pair. --

Please replace the paragraph beginning on page 8, line 9, with the following amended paragraph:

-- In this solution the following assumptions are made. The mobile phone's Security Identity Module (SIM) card-signed PGP® key packet only "lives" for a short time (a few minutes) in the system and is then thrown away. If it is logged it can be used for journalizing the transactions in the issuing process. Also it can be logged perhaps for keeping track of errors. If there were to be any permanent retention of this packet (for legal or other purposes), it would have to comply with some existing standard format, in order to be assured that it could be accessed and correctly interpreted in the future. --

Please replace the paragraph beginning on page 8, line 20, with the following amended paragraph:

-- As described here, the format of the phone-signed PGP® key packet does not fit any existing standard. If necessary, a standard format could be designed, and the SIM card software would be required to create signatures in this format. The user has control (physical security) of the PC and corresponding PGP® private key used for performing the operations described here. The CA operates a publicly accessible PGP® keyserver containing all of the PGP® keys that the CA has signed. --

Please replace the paragraph beginning on page 8, line 30, with the following amended paragraph:

-- Here we describe the steps to follow in order to use the applicants S3 system to securely sign a PGP® key by the WPKI CA (WPKI, Wireless public key infrastructure), using a user's S3 SIM card to link the signature back to the proof of identity that was presented to the WPKI Local Registration Authority. This process is performed without breaching the anonymity of the user's SIM card Network ID (NID). As described here, the process is stateless on the CA end, reducing complexity and increasing resiliency of the protocol for the CA. --

Please replace the paragraph beginning on page 9, line 3, with the following amended paragraph:

-- At first software using PGP® on the PC displays the name and PGP® key fingerprint of the user that is to be certified on the PC screen. Also displayed on the PC display is a prompt to enter the 4 digit number on the mobile phone display. --

Please replace the paragraph beginning on page 9, line 8, with the following amended paragraph:

-- The PGP® key fingerprint is a cryptographically strong hash of the key. PGP® users are accustomed to verifying keys by comparing key fingerprints so this makes it easier to verify the ~~PC-Phone~~ link between the PC and the Phone is reliable, and not being attacked by an intruder inserting a take message to be signed by the phone. The latter is probably not necessary to protect against, since we assume physical security for that link. However, the link is not necessarily secured. --

Please replace the paragraph beginning on page 9, line 17, with the following amended paragraph:

-- The PC software communicates with the phone through the wired or wireless interface or other appropriate interface, and passes a message packet ~~(TBD)~~ containing a command to start the PGP® key signing process. Phone generates and displays a four digit random number, along with a prompt to type this number into the PC if the user wants to sign his PGP® key with his phone key. --

Please replace the paragraph beginning on page 10, line 4, with the following amended paragraph:

-- The phone compares the random number sent with the "What is my name?" request, and if it matches, displays a warning that it is about to sign a PGP® key with its key. --

Please replace the paragraph beginning on page 10, line 8, with the following amended paragraph:

-- PC displays a lengthy legal notice to user warning that user is about to sign their PGP® key with the phone's key and that the user is contractually obligated to only make this signature if he is the owner of both keys. Again, if the random number matched, the "What is my name?" message is signed by the phone, returned to the PC through the serial interface, and saved for transmission to the CA. The PC software generates another message, intended for transmission to the CA, this message contains the key fingerprint, and a request to the CA to sign the attached key, if the fingerprint matches. This is a "Sign this User ID and key, please." request. The "Sign this User ID and key, please." message is then passed to the phone through

the serial interface, with a request that the phone sign the packet, using the its SIM card private key. --

Please replace the paragraph beginning on page 10, line 24, with the following amended paragraph:

-- The PGP® key fingerprint is displayed on the phone at this point and verified, by the user to be in agreement with the PGP® key fingerprint on the PC screen. The user is prompted to OK the signature, if the fingerprint matches. The User's phone sends the signed "Sign this User ID and key, please." packet back through the serial interface to the PC (along with the phone key ID that signed it). Save on the PC for later transmission to the CA. The ~~PC-Phone~~ connection between the PC and the phone is no longer needed after this point, and is dropped. --

Please replace the paragraph beginning on page 10, line 34, with the following amended paragraph:

-- Note that if desired, the process described in the preceding few steps could be accomplished with only one signed message from the phone. This message would contain a signature of the PGP® key fingerprint. The one message would be used with two different meanings, first to ask the CA, "What's my User ID (name)?", and second to command it to "Sign this Key and User ID please". In the first case the PGP® key fingerprint is ignored, since only the phone's NID is need to specify what name is desired from the CA. --

Please replace the paragraph beginning on page 11, line 7, with the following amended paragraph:

-- The PC opens up a secure channel (using Transport Layer Security (TLS)) to the Certification Authority. The PC sends the SIM signed request for User ID ("What's my User ID and name?") query to the CA over the secure link. --

Please replace the paragraph beginning on page 11, line 11, with the following amended paragraph:

-- The CA looks up the phone's owner in the confidential database, and sends the User ID for the phone back to the PC, as requested. This is the WPKI User ID that the phone's owner had certified at the Local Registration Authority (LRA). Sending this information to the PC does not breach the anonymity of the NID, since the link is encrypted and the phone owner is the one making the request. --

Please replace the paragraph beginning on page 11, line 18, with the following amended paragraph:

-- The PC checks to see if the returned WPKI User ID is present on the users PGP® key. If it is, then the process proceeds to the next step, automatically. If the returned WPKI User ID is not present on the PGP® key, then the User ID is added to the PGP® key before proceeding. --

Please replace the paragraph beginning on page 11, line 24, with the following amended paragraph:

-- If the WPKI User ID must be added to the PGP® key, we branch off at this point and follow the normal PGP® procedure for adding a new User ID to one's key-ring. The user must supply an email address for this User ID, because the User ID supplied by the CA wall not have an email address. --

Please replace the paragraph beginning on page 11, line 30, with the following amended paragraph:

-- Since the ultimate result of this process will be publication of the signed key on a public keyserver, the User ID must be self-signed. PGP® User IDs are only suitable for publication it they are signed by the key's owner. --

Please replace the paragraph beginning on page 11, line 35, with the following amended paragraph:

-- The PC next uses the user's PGP® private key to sign the "Sign this key, please." request to the CA (this request is asking the CA to sign the phone owner's PGP® key, remember). This request was signed earlier by the phone's SIM card. --

Please replace the paragraph beginning on page 12, line 7, with the following amended paragraph:

-- The PC sends the PGP® and Phone signed "Sign this User ID and Key, Please." request packet with the corresponding PGP® key up to the CA, through the established TLS link.

Again, this packet links the phone owner's (presumably anonymous) NID with the public PGP® identity, so the channel must be encrypted. --

Please replace the paragraph beginning on page 12, line 21, with the following amended paragraph:

-- If the submitted User ID for this phone is not found in the CA's confidential database, the request is denied, and an error message is sent back to the PC. For debugging purposes, this error message could contain the correct User ID, since we are operating over an encrypted channel. The user is informed of the problem via an error message displayed on PC. If the name portion of the user IDs match, then the CA signs the PGP® key with the CA key and discards the "Sign this key, Please" request with the phone NID. It then inserts this information into the confidential database. The CA-signed PGP® key is added to a "Pending PGP® Certificate" database on the CA. --

Please replace the paragraph beginning on page 13, line 5, with the following amended paragraph:

-- The CA expects the user to decrypt and re-upload the signed key back up to the CA, thus proving that the email address was correct, and the person residing at that email address has the capability of decrypting with that key. When the CA receives this key back from the user, the CA purges it from the Pending PGP® Certificate database. To overcome email delivery problems, periodically the CA will repeat the previous step until the user responds or until the CA decides to give up. --

Please replace the paragraph beginning on page 13, line 15, with the following amended paragraph:

-- When the CA receives this key back from the user, the CA publishes the resultant signed PGP® key on its PGP® key server. The PGP® key is signed only with the LRA-verified User ID, of course. None of the other UserIDs that the user might have on his PGP® key are signed by the CA. Note also that the telephone NID is not part of the PGP® key, nor is it published with the PGP® key, so we are still protecting the user's NID-related anonymity. --

Please replace the paragraph beginning on page 14, line 10, with the following amended paragraph:

-- Figure 3 presents one example of the certificate of the present invention. The certificate contains a number of information, which are required for the identification. Typically such information are certificate identification number, user name, users e-mail address, RSA/Digital Signature Scheme (RSA/DSS) keys, the fingerprint of the signature or of the certificate itself, the hash of the passphrase, the signature, and the expiration date of the certificate.